プラットフォーム設定

管理 IP アドレスの変更

はじめる前に

FXOS CLI から FXOS シャーシの管理 IP アドレスを変更できます。

（注） 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

手順

ステップ 1 FXOS CLI に接続します（FXOS CLI へのアクセスを参照）。

ステップ 2 IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。

Firepower-chassis# **scopefabric-interconnecta**

b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect # **show**

c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect #
setout-of-bandip*ip_address***netmask***network_mask***gw***gateway_ip_address*

d) トランザクションをシステム設定にコミットします。
Firepower-chassis /fabric-interconnect* # **commit-buffer**

ステップ 3 IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。
Firepower-chassis# **scopefabric-interconnecta**

b) 管理 IPv6 設定のスコープを設定します。
Firepower-chassis /fabric-interconnect # **scopeipv6-config**

c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect/ipv6-config #
setout-of-bandipv6*ipv6_address***ipv6-prefix***prefix_length***ipv6-gw***gateway_address*

e) トランザクションをシステム設定にコミットします。
Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ ------------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                      Prefix     IPv6 Gateway
    --------------------------------- ---------- ------------
    2001::8998                        64         2001::1
```

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

日時の設定

手動で日時を設定するか、NTP サーバを設定するには、（以下に説明する CLI コマンド）を使用します。

（注） NTP の設定は、Firepower シャーシとシャーシに設置されたアプリケーション間では同期されません。適切な機能を確保するために、Firepower シャーシとシャーシで稼動するアプリケーションに同じ NTP 設定を構成する必要があります。

タイム ゾーンの設定

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 タイム ゾーンを設定します。
Firepower-chassis /system/services # **settimezone**

この時点で、大陸、国、およびタイム ゾーン領域に対応する番号を入力するように求められます。プロンプトごとに適切な情報を入力します。

ロケーション情報の指定を完了すると、プロンプトが表示され、正しいタイム ゾーン情報が設定されているか確認するよう求められます。確認する場合は 1（yes）を入力し、操作をキャンセルする場合は 2（no）を入力します。

ステップ 4 設定されたタイム ゾーンを表示する場合：
Firepower-chassis /system/services # **top**
Firepower-chassis# **show timezone**

次に、太平洋標準時領域にタイム ゾーンを設定し、トランザクションをコミットし、設定したタイム ゾーンを表示する例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
```

```
1) Africa           4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas         5) Asia             8) Europe
3) Antarctica       6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2015.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2015.
```

```
Is the above information OK?
1) Yes
2) No
#? 1
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services # top
Firepower-chassis# show timezone
Timezone: America/Los_Angeles (Pacific Time)
Firepower-chassis#
```

NTP サーバの追加

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 指定したホスト名、IPv4 または IPv6 アドレスの NTP サーバを使用するようにシステムを設定します。
Firepower-chassis /system/services # **createntp-server***{hostname | ip-addr | ip6-addr}*

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower-chassis /system/services # **commit-buffer**

次の例では、IP アドレス 192.168.200.101 を持つNTP サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IPv6 アドレス 4001::6 を持つ NTP サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

NTP サーバの削除

手順

ステップ 1 システム モードに入ります。
Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 指定したホスト名、IPv4 または IPv6 アドレスの NTP サーバを削除します。
Firepower-chassis /system/services # **deletentp-server***{hostname | ip-addr | ip6-addr}*

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower-chassis /system/services # **commit-buffer**

次に、IP アドレス 192.168.200.101 の NTP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次に、IPv6 アドレス 4001::6 の NTP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

手動での日付と時刻の設定

ここでは、Firepower シャーシで日付と時刻を手動で設定する方法について説明します。システム クロックの変更はただちに反映されます。

（注） システム クロックが NTP サーバと同期中である場合は、日付と時刻を手動で設定することはできません。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scopesystem**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system # **scopeservices**

ステップ 3 システム クロックを設定します。
Firepower-chassis /system/services # **set clock** *month day year hour min sec*

month には、月の英名の最初の 3 文字を使用します。時間は 24 時間形式で入力する必要があります。午後 7 時は 19 になります。

システム クロックの変更はただちに反映されます。バッファをコミットする必要はありません。

次に、システム クロックを設定する例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set clock jun 24 2015 15 27 00
Firepower-chassis /system/services #
```

SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効化またはディセーブルにする方法について説明します。SSH はデフォルトでイネーブルになります。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 Firepower シャーシへの SSH アクセスを設定するには、次のいずれかを実行します。

- Firepower シャーシへの SSH アクセスを許可するには、次のコマンドを入力します。
  Firepower-chassis /system/services # **enable ssh-server**
- Firepower シャーシへの SSH アクセスを禁止するには、次のコマンドを入力します。
  Firepower-chassis /system/services # **disable ssh-server**

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower /system/services # **commit-buffer**

次の例では、Firepower シャーシへの SSH アクセスを有効化し、トランザクションをコミットします。

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # enable ssh-server
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Telnet の設定

次の手順では、Firepower シャーシへの Telnet アクセスを有効化またはディセーブルにする方法について説明します。Telnet はデフォルトでディセーブルです。

（注） 現在は、CLI を使用した Telnet 設定のみ可能です。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 Firepower シャーシへの Telnet アクセスを設定するには、次のいずれかを実行します。

- Firepower シャーシへの Telnet アクセスを許可するには、次のコマンドを入力します。
  Firepower-chassis /system/services # **enable telnet-server**
- Firepower シャーシへの Telnet アクセスを禁止するには、次のコマンドを入力します。
  Firepower-chassis /system/services # **disable telnet-server**

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower /system/services # **commit-buffer**

次に、Telnet を有効にし、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

SNMP の設定

ここでは、Firepower シャーシに簡易ネットワーク管理プロトコル（SNMP）を設定する方法について説明します。詳細については、次のトピックを参照してください。

SNMP の概要

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーション レイヤ プロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：Firepower シャーシ内のソフトウェア コンポーネントで、Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに送信します。Firepower シャーシには、エージェントと一連の MIB が含まれています。SNMP エージェントを有効化にしてマネージャとエージェント間のリレーションシップを作成するには、Firepower Chassis Manager または FXOS CLI で SNMP を有効化して設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。SNMP は次のように定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Firepower シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Firepower シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。Firepower シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルは、選択したセキュリティ レベルと結合され、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *1*：*SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	Community string	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	Community string	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	Username	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	No	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。SNMPv3 ユーザベース セキュリティ モデル（USM） は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

MIB のサポート

Firepower シャーシは MIB への読み取り専用アクセスをサポートします。

SNMPv3 ユーザの認証プロトコル

Firepower シャーシは、SNMPv3 ユーザの HMAC-SHA-96（SHA）認証プロトコルをサポートします。

SNMPv3 ユーザの AES プライバシー プロトコル

Firepower シャーシは、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効化して、SNMPv3 ユーザのプライバシー パスワードを含めると、Firepower シャーシはそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。AES プライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP のイネーブル化および SNMP プロパティの設定

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP をイネーブルにします。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 SNMP コミュニティ モードを開始します。
Firepower-chassis /monitoring # **set snmp community**

set snmp community コマンドを入力すると、SNMP コミュニティの入力を求められます。

ステップ 4 SNMP コミュニティを指定します。パスワードとしてコミュニティ名を使用します。コミュニティ名は、最大 32 文字の英数字で指定できます。
Firepower-chassis /monitoring # **Enter a snmp community:***community-name*

ステップ 5 SNMP 担当者のシステムの連絡先を指定します。システムの連絡先名（電子メール アドレスや、名前と電話番号など）は、最大 255 文字の英数字で指定できます。
Firepower-chassis /monitoring # **set snmp syscontact***system-contact-name*

ステップ 6 SNMP エージェント（サーバ）が実行されるホストの場所を指定します。システム ロケーション名は、最大 512 文字の英数字で指定できます。
Firepower-chassis /monitoring # **set snmp syslocation***system-location-name*

ステップ 7 トランザクションをシステム設定にコミットします。
Firepower-chassis /monitoring # **commit-buffer**

次に、SNMP をイネーブルにし、SnmpCommSystem2 という名前の SNMP コミュニティを設定し、contactperson という名前のシステム連絡先を設定し、systemlocation という名前の連絡先ロケーションを設定し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
Firepower-chassis /monitoring* # set snmp syscontact contactperson1
Firepower-chassis /monitoring* # set snmp syslocation systemlocation
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

次の作業

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP をイネーブルにします。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 指定したホスト名、IPv4 アドレス、または IPv6 アドレスで SNMP トラップを作成します。
Firepower-chassis /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}

ステップ 4 SNMP トラップに使用する SNMP コミュニティ名を指定します。
Firepower-chassis /monitoring/snmp-trap # **set community** *community-name*

ステップ 5 SNMP トラップに使用するポートを指定します。
Firepower-chassis /monitoring/snmp-trap # **set port***port-num*

ステップ 6 トラップに使用する SNMP のバージョンとモデルを指定します。
Firepower-chassis /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}

ステップ 7 （任意） 送信するトラップのタイプを指定します。
Firepower-chassis /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}

ここに表示される値は次のとおりです。

- バージョンで v2c または v3 を選択した場合は **traps**。
- バージョンで v2c を選択した場合は **informs**。

（注） バージョンで v2c を選択した場合にのみインフォーム通知を送信できます。

ステップ 8 （任意） バージョンで v3 を選択した場合は、トラップに関連付ける権限を指定します。
Firepower-chassis /monitoring/snmp-trap # **set v3privilege** {**auth** | **noauth** | **priv**}

ここに表示される値は次のとおりです。

- [auth]：認証あり、暗号化なし
- [noauth]：認証なし、暗号化なし
- [priv]：認証あり、暗号化あり

ステップ 9 トランザクションをシステム設定にコミットします。
Firepower-chassis /monitoring/snmp-trap # **commit-buffer**

次の例は、SNMP をイネーブルにし、IPv4 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem2 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 192.168.100.112
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem2
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

次の例は、SNMP をイネーブルにし、IPv6 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem3 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 2001::1
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem3
Firepower-chassis /monitoring/snmp-trap* # set port 2
```

```
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

SNMP トラップの削除

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 指定したホスト名または IP アドレスの SNMP トラップを削除します。
Firepower-chassis /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}

ステップ 3 トランザクションをシステム設定にコミットします。
Firepower-chassis /monitoring # **commit-buffer**

次に、IP アドレス 192.168.100.112 で SNMP トラップを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-trap 192.168.100.112
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

SNMPv3 ユーザの作成

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 SNMP をイネーブルにします。
Firepower-chassis /monitoring # **enable snmp**

ステップ 3 指定した SNMPv3 ユーザを作成します。
Firepower-chassis /monitoring # **create snmp-user***user-name*

create snmp-user コマンドを入力すると、パスワードの入力を促すプロンプトが表示されます。

ステップ 4 AES-128 暗号化の使用を有効化またはディセーブルにします。
Firepower-chassis /monitoring/snmp-user # **set aes-128** {**no** | **yes**}

デフォルトでは、AES-128 暗号化はディセーブルになっています。

ステップ 5 ユーザ プライバシー パスワードを指定します。

Firepower-chassis /monitoring/snmp-user # **set priv-password**

set priv-password コマンドを入力すると、プライバシー パスワードの入力と確認を促すプロンプトが表示されます。

ステップ 6 トランザクションをシステム設定にコミットします。
Firepower-chassis /monitoring/snmp-user # **commit-buffer**

次の例では、SNMP を有効化し、snmp-user14 という名前の SNMPv3 ユーザを作成し、AES-128 暗号化を有効化し、パスワードおよびプライバシー パスワードを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-user snmp-user14
Password:
Firepower-chassis /monitoring/snmp-user* # set aes-128 yes
Firepower-chassis /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
Firepower-chassis /monitoring/snmp-user* # commit-buffer
Firepower-chassis /monitoring/snmp-user #
```

SNMPv3 ユーザの削除

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 指定した SNMPv3 ユーザを削除します。
Firepower-chassis /monitoring # **delete snmp-user***user-name*

ステップ 3 トランザクションをシステム設定にコミットします。
Firepower-chassis /monitoring # **commit-buffer**

次に、snmp user14 という名前の SNMPv3 ユーザを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-user snmp-user14
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

HTTPS ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 HTTPS 接続に使用するポートを指定します。
Firepower-chassis /system/services # **sethttpsport***port-number*

port-number には 1 ～ 65535 の整数を指定します。HTTPS は、デフォルトでポート 443 で有効化になります。

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower /system/services # **commit-buffer**

HTTPS ポートを変更すると、現在のすべての HTTPS セッションが閉じられます。ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

<*chassis_mgmt_ip_address*> は、初期設定時に入力した Firepower シャーシの IP アドレスまたはホスト名で、<*chassis_mgmt_port*> は設定が完了した HTTPS ポートです。

次の例では、HTTPS ポート番号を 443 に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set https port 444
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

AAA の設定

ここでは、認証、認可、アカウンティングについて説明します。詳細については、次のトピックを参照してください。

AAA について

AAA は、コンピュータ リソースへのアクセスの制御、ポリシーの適用、使用状況の評価することでサービスの課金に必要な情報を提供する、一連のサービスです。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレ

デンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合、認証は失敗し、ネットワーク アクセスは拒否されます。

FXOS シャーシ では、次のセッションを含むシャーシへの管理接続を認証するように設定することができます。

- HTTPS
- SSH
- シリアル コンソール

認証

認可はポリシーを使用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。そこには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティ プランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA サーバ

AAA サーバは、アクセス コントロールに使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

ローカル データベースのサポート

Firepower シャーシは、ユーザ プロファイルを取り込むことができるローカル データベースを維持します。AAA サーバの代わりにローカルデータベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 指定した属性を含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set attribute** *attribute*

ステップ 4 指定した識別名を含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set basedn** *distinguished-name*

ステップ 5 指定したフィルタを含むレコードにデータベース検索を限定します。
Firepower-chassis /security/ldap # **set filter** *filter*

ステップ 6 システムがサーバをダウン状態として通知する前に、LDAP サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/ldap # **set timeout** *seconds*

ステップ 7 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/ldap # **commit-buffer**

次の例では、LDAP 属性を CiscoAvPair に、ベース識別名を「DC=cisco-firepower-aaa3,DC=qalab,DC=com」に、フィルタを sAMAccountName=$userid に、タイムアウト間隔を 5 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # set attribute CiscoAvPair
Firepower-chassis /security/ldap* # set basedn "DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap* # set filter sAMAccountName=$userid
Firepower-chassis /security/ldap* # set timeout 5
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

（注） ユーザ ログインは LDAP ユーザの userdn が 255 文字を超えると失敗します。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の LDAP プロバイダーがサポートされます。

はじめる前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 LDAP サーバ インスタンスを作成し、セキュリティ LDAP サーバ モードを開始します。
Firepower-chassis /security/ldap # **create server***server-name*

SSL が有効化の場合、*server-name* は、通常 IP アドレスまたは FQDN となり、LDAP サーバのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。IP アドレスが指定されていない場合は、DNS サーバを設定する必要があります。

ステップ 4 （任意） ユーザ ロールとロケールの値を保管する LDAP 属性を設定します。
Firepower-chassis /security/ldap/server # **set attribute***attr-name*

このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。

デフォルトの属性が LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 5 （任意） リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名を設定します。
Firepower-chassis /security/ldap/server # **set basedn***basedn-name*

ベース DN の長さは、最大 255 文字から CN=username の長さを引いた長さに設定することができます。username により、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI にアクセスしようとするリモート ユーザが識別されます。

デフォルトのベース DN が LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 6 （任意） ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）を設定します。
Firepower-chassis /security/ldap/server # **set binddn***binddn-name*

サポートされるストリングの最大長は 255 文字（ASCII）です。

ステップ 7 （任意） LDAP 検索を、定義されたフィルタと一致するユーザ名に制限します。
Firepower-chassis /security/ldap/server # **set filter***filter-value*

デフォルトのフィルタが LDAP プロバイダーに対して設定されていない場合は、この値が必要です。

ステップ 8 バインド DN に指定した LDAP データベース アカウントのパスワードを指定します。
Firepower-chassis /security/ldap/server # **set password**

標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。

パスワードを設定するには、**set password** コマンドを入力してから **Enter** キーを押し、プロンプトでキー値を入力します。

ステップ 9 （任意） Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序を指定します。
Firepower-chassis /security/ldap/server # **set order***order-num*

ステップ 10 （任意） LDAP サーバとの通信に使用するポートを指定します。標準ポート番号は 389 です。
Firepower-chassis /security/ldap/server # **set port***port-num*

ステップ 11 LDAP サーバと通信するときの暗号化の使用を有効化またはディセーブルにします。
Firepower-chassis /security/ldap/server # **set ssl** {**yes**|**no**}

オプションは次のとおりです。

- **yes**：暗号化が必要です。暗号化をネゴシエートできない場合は、接続に失敗します。
- **no**：暗号化はディセーブルです。認証情報はクリア テキストとして送信されます。

LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。

ステップ 12 LDAP データベースへの問い合わせがタイム アウトするまでの秒数を指定します。
Firepower-chassis /security/ldap/server # **set timeout***timeout-num*

1～60 秒の整数を入力するか、0（ゼロ）を入力して LDAP プロバイダーに対して指定したグローバル タイムアウト値を使用します。デフォルトは 30 秒です。

ステップ 13 LDAP プロバイダーまたはサーバの詳細を提供するベンダーを指定します。
Firepower-chassis /security/ldap/server # **set vendor***{ms-ad | openldap}*

オプションは次のとおりです。

- **ms-ad**：LDAP プロバイダーは Microsoft Active Directory です。
- **openldap**：LDAP プロバイダーは Microsoft Active Directory ではありません。

ステップ 14 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/ldap/server # **commit-buffer**

次の例では、10.193.169.246 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 10.193.169.246
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 2
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 30
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

次の例では、12:31:71:1231:45b1:0011:011:900 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 1
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 45
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

LDAP プロバイダーの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ LDAP モードを開始します
Firepower-chassis /security # **scope ldap**

ステップ 3 指定したサーバを削除します。
Firepower-chassis /security/ldap # **delete server** *serv-name*

ステップ 4 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/ldap # **commit-buffer**

次に、ldap1 という名前の LDAP サーバを削除し、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # delete server ldap1
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope radius**

ステップ 3 （任意） サーバをダウン状態として通知する前に RADIUS サーバとの通信を再試行する回数を指定します。
Firepower-chassis /security/radius # **set retries** *retry-num*

ステップ 4 （任意） システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/radius # **set timeout** *seconds*

ステップ 5 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/radius # **commit-buffer**

次の例は、RADIUS リトライを 4 に設定し、タイムアウト間隔を 30 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # set retries 4
Firepower-chassis /security/radius* # set timeout 30
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の RADIUS プロバイダーがサポートされます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope radius**

ステップ 3 RADIUS サーバ インスタンスを作成し、セキュリティ RADIUS サーバ モードを開始します。
Firepower-chassis /security/radius # **create server***server-name*

ステップ 4 （任意） RADIUS サーバとの通信に使用するポートを指定します。
Firepower-chassis /security/radius/server # **set authport***authport-num*

ステップ 5 RADIUS サーバ キーを設定します。
Firepower-chassis /security/radius/server # **set key**

キー値を設定するには、**set key** コマンドを入力してから Enter キーを押し、プロンプトでキー値を入力します。

ステップ 6 （任意） このサーバが試行される順序を指定します。
Firepower-chassis /security/radius/server # **set order** *order-num*

ステップ 7 （任意） サーバをダウン状態として通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
Firepower-chassis /security/radius/server # **set retries** *retry-num*

ステップ 8 システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を指定します。
Firepower-chassis /security/radius/server # **set timeout** *seconds*

ヒント RADIUS プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。

ステップ 9 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/radius/server # **commit-buffer**

次の例は、radiusserv7 という名前のサーバインスタンスを作成し、認証ポートを 5858 に設定し、キーを radiuskey321 に設定し、順序を 2 に設定し、再試行回数を 4 回に設定し、タイムアウトを 30 に設定し、二要素認証をイネーブルにし、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
```

```
Firepower-chassis /security/radius # create server radiusserv7
Firepower-chassis /security/radius/server* # set authport 5858
Firepower-chassis /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
Firepower-chassis /security/radius/server* # set order 2
Firepower-chassis /security/radius/server* # set retries 4
Firepower-chassis /security/radius/server* # set timeout 30
Firepower-chassis /security/radius/server* # commit-buffer
Firepower-chassis /security/radius/server #
```

RADIUS プロバイダーの削除

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ RADIUS モードを開始します
Firepower-chassis /security # **scope RADIUS**

ステップ 3 指定したサーバを削除します。
Firepower-chassis /security/radius # **delete server** *serv-name*

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/radius # **commit-buffer**

次の例は、radius1 という RADIUS サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # delete server radius1
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3 （任意） システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。
Firepower-chassis /security/tacacs # **set timeout** *seconds*

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower-chassis /security/tacacs # **commit-buffer**

次の例は、TACACS+ タイムアウト間隔を 45 秒に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # set timeout 45
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の TACACS+ プロバイダーがサポートされます。

手順

ステップ 1 セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2 セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3 TACACS+ サーバ インスタンスを作成し、TACACS+ サーバ モードを開始します。
Firepower-chassis /security/tacacs # **create server** *server-name*

ステップ 4 TACACS+ サーバ キーを指定します。
Firepower-chassis /security/tacacs/server # **set key**

キー値を設定するには、**set key** コマンドを入力してから Enter キーを押し、プロンプトでキー値を入力します。

ステップ 5 （任意） このサーバが試行される順序を指定します。
Firepower-chassis /security/tacacs/server # **set order***order-num*

ステップ 6 システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を指定します。
Firepower-chassis /security/tacacs/server # **set timeout***seconds*

ヒント　TACACS+ プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。

ステップ 7　（任意）　TACACS+ サーバとの通信に使用するポートを指定します。
Firepower-chassis /security/tacacs/server # **set port***port-num*

ステップ 8　トランザクションをシステム設定にコミットします。
Firepower-chassis /security/tacacs/server # **commit-buffer**

次の例は、tacacsserv680 という名前のサーバ インスタンスを作成し、キーを tacacskey321 に設定し、順序を 4 に設定し、認証ポートを 5859 に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # create server tacacsserv680
Firepower-chassis /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
Firepower-chassis /security/tacacs/server* # set order 4
Firepower-chassis /security/tacacs/server* # set port 5859
Firepower-chassis /security/tacacs/server* # commit-buffer
Firepower-chassis /security/tacacs/server #
```

TACACS+ プロバイダーの削除

手順

ステップ 1　セキュリティ モードを開始します。
Firepower-chassis# **scope security**

ステップ 2　セキュリティ TACACS+ モードを開始します。
Firepower-chassis /security # **scope tacacs**

ステップ 3　指定したサーバを削除します。
Firepower-chassis /security/tacacs # **delete server** *serv-name*

ステップ 4　トランザクションをシステム設定にコミットします。
Firepower-chassis /security/tacacs # **commit-buffer**

次の例では、tacacs1 という TACACS+ サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # delete server tacacs1
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

Syslog の設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

手順

ステップ 1 モニタリング モードを開始します。
Firepower-chassis# **scope monitoring**

ステップ 2 コンソールへの syslog の送信を有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog console**

ステップ 3 （任意） 表示するメッセージの最低レベルを選択します。syslog がイネーブルの場合、システムはそのレベル以上のメッセージをコンソールに表示します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}

ステップ 4 オペレーティング システムによる syslog 情報のモニタリングを有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog monitor**

ステップ 5 （任意） 表示するメッセージの最低レベルを選択します。モニタの状態がイネーブルの場合、システムはそのレベル以上のメッセージを表示します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

（注） Critical より下のレベルのメッセージは、**terminal monitor** コマンドを入力した場合にのみ端末モニタに表示されます。

ステップ 6 syslog ファイルへの syslog 情報の書き込みを有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog file**

ステップ 7 メッセージが記録されるファイルの名前を指定します。ファイル名は16文字まで入力できます。
Firepower-chassis /monitoring # **set syslog file name***filename*

ステップ 8 （任意） ファイルに保存するメッセージの最低レベルを選択します。ファイルの状態がイネーブルの場合、システムはそのレベル以上のメッセージを syslog ファイルに保存します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

ステップ 9 （任意） 最新のメッセージで最も古いメッセージが上書きされる前の最大ファイル サイズ（バイト単位）を指定します。有効な範囲は 4096 ～ 4194304 バイトです。

Firepower-chassis /monitoring # **set syslog file size***filesize*

ステップ 10 最大 3 台の外部 syslog サーバへの syslog メッセージの送信を設定します。

a) 最大 3 台の外部 syslog サーバへの syslog メッセージの送信を有効化またはディセーブルにします。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}

b) （任意） 外部ログに保存するメッセージの最低レベルを選択します。remote-destination がイネーブルにされると、システムはそのレベル以上を外部サーバに送信します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level**{**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

c) 指定したリモート syslog サーバのホスト名または IP アドレスを指定します。ホスト名は 256 文字まで入力できます。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname***hostname*

d) （任意） 指定したリモート syslog サーバに送信される syslog メッセージに含まれるファシリティ レベルを指定します。
Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}

ステップ 11 ローカル送信元を設定します。有効化またはディセーブルにするローカル送信元ごとに、次のコマンドを入力します。
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}

次のいずれかになります。

- audits：すべての監査ログ イベントのロギングを有効化またはディセーブルにします。
- events：すべてのシステム イベントのロギングを有効化またはディセーブルにします。
- faults：すべてのシステム障害のロギングを有効化またはディセーブルにします。

ステップ 12 トランザクションをコミットします。
Firepower-chassis /monitoring # **commit-buffer**

次の例は、ローカル ファイルの syslog メッセージのストレージをイネーブルにし、トランザクションをコミットします。

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # disable syslog console
Firepower-chassis /monitoring* # disable syslog monitor
Firepower-chassis /monitoring* # enable syslog file
Firepower-chassis /monitoring* # set syslog file name SysMsgsFirepower
Firepower-chassis /monitoring* # set syslog file level notifications
Firepower-chassis /monitoring* # set syslog file size 4194304
Firepower-chassis /monitoring* # disable syslog remote-destination server-1
Firepower-chassis /monitoring* # disable syslog remote-destination server-2
Firepower-chassis /monitoring* # disable syslog remote-destination server-3
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。たとえば、DNS サーバを設定していないと、Firepower シャーシで設定を行うときに、www.cisco.com などの名前を使用できません。サーバの IP アドレスを使用する必要があり、IPv4 または IPv6 アドレスのいずれかを使用できます。最大 4 台の DNS サーバを設定できます。

（注） 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

手順

ステップ 1 システム モードに入ります。
Firepower-chassis #**scope system**

ステップ 2 システム サービス モードを開始します。
Firepower-chassis /system #**scope services**

ステップ 3 DNS サーバを作成または削除するには、次の該当するコマンドを入力します。

- 指定した IPv4 または IPv6 アドレスの DNS サーバを使用するようにシステムを設定する場合：

  Firepower-chassis /system/services # **createdns***{ip-addr* | *ip6-addr}*

- 指定した IPv4 または IPv6 アドレスの DNS サーバを削除する場合：

  Firepower-chassis /system/services # **deletedns***{ip-addr* | *ip6-addr}*

ステップ 4 トランザクションをシステム設定にコミットします。
Firepower /system/services # **commit-buffer**

次の例では、IPv4 アドレス 192.168.200.105 を持つ DNS サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IPv6 アドレス 2001:db8::22:F376:FF3B:AB3F を持つ DNS サーバを設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
```

```
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

次の例では、IP アドレス 192.168.200.105 を持つ DNS サーバを削除し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```